Strategy Research Project

THE OBSOLESCENCE OF DMS IN AN INFORMATION CENTRIC WORLD

BY

COLONEL EDWARD C. PREM
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-04-2011	Strategy Research Project	

4. TITLE AND SUBTITLE
The Obsolescence of DMS in an Information Centric World

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Edward C. Prem

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Robert W. Hoelscher
Chief Information Officer

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The current organizational messaging capability within the Department of Defense (DoD) is an old technology operating on a system centric paradigm. The system centric methodology for transmitting organizational messages is obsolete in the information centric in which world we live. The importance of the information should determine what requirements are levied against it instead of a system imposing all requirements on every message. It is the information contained within an organizational message that is important; not the fact that it was transmitted from a particular system. In order to modernize organizational messaging it must shift to information centric versus a system centric paradigm. Messaging in an information centric paradigm is cheaper to maintain, flexible, easier to modify and share with the unintended user. In today's world messaging is about the information, not the system.

15. SUBJECT TERMS
Organizational Messaging

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	26	

USAWC STRATEGY RESEARCH PROJECT

THE OBSOLESCENCE OF DMS IN AN INFORMATION CENTRIC WORLD

by

Colonel Edward C. Prem
United States Army

Colonel Robert W. Hoelscher
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Edward C. Prem

TITLE: The Obsolescence of DMS in an Information Centric World

FORMAT: Strategy Research Project

DATE: 13 April 2011 WORD COUNT: 5,163 PAGES: 26

KEY TERMS: Organizational Messaging

CLASSIFICATION: Unclassified

The current organizational messaging capability within the Department of Defense (DoD) is an old technology operating on a system centric paradigm. The system centric methodology for transmitting organizational messages is obsolete in the information centric in which world we live. The importance of the information should determine what requirements are levied against it instead of a system imposing all requirements on every message. It is the information contained within an organizational message that is important; not the fact that it was transmitted from a particular system. In order to modernize organizational messaging it must shift to information centric versus a system centric paradigm. Messaging in an information centric paradigm is cheaper to maintain, flexible, easier to modify and share with the unintended user. In today's world messaging is about the information, not the system.

THE OBSOLESCENCE OF DMS IN AN INFORMATION CENTRIC WORLD

> The Joint Staff intends to eliminate DMS in fiscal year 2009 and employ alternative mechanisms for the transfer of Official Information (OI). The tools currently available for use include wikis, blogs, chat, and individual e-mail using public key infrastructure certificates. … Organizations should look for other methods and are not constrained or confined by CJCSI 5721.01D to utilize DMS. … We have a great opportunity to streamline and simplify the way we transfer official information, and I encourage you to be a part of the solution.
>
> —James E. Cartwright[1]

The requirement for an organizational messaging capability has existed since armies first clashed. Runners between units or cities carried command and control messages or news of victory or defeat. The most famous example being the 26 mile run from the battle of Marathon back to Athens with news of Miltiades victory over the Persian army led by Datis. Signal fires and flags served the same purpose. The advent of the telegraph revolutionized messaging. Messages could be sent in near real time across great distances. Innovations in the telecommunications industry continued to improve the speed and effectiveness of messaging with each new technology supplanting its predecessor. Such was the case with electronic mail, or email. Email was rapidly adopted as the new standard both in industry and the military for messaging. Historically, new and better technologies must eventually replace the old.

The current organizational messaging capability within the Department of Defense (DoD) uses 1980s technology operating on a system centric paradigm. The system centric methodology for transmitting organizational messages is obsolete in the information centric world we live in. It is the information contained within an organizational message that is important; not the fact that it was transmitted from a particular system. The importance of the information should determine what

requirements are levied against it instead of a system imposing all requirements on every message. In order to modernize organizational messaging it must shift to information centric from a system centric paradigm. Using an information centric paradigm for messaging is cheaper to maintain, flexible, easier to modify and share with the unintended user. In today's world messaging is about the information, not the system.

Defense Message System

While there are many new technologies and better transmission methods the Department of Defense (DoD) continues to use its antiquated Defense Message System (DMS). What is the Defense Message System? DMS is a Department of Defense (DoD) program initiated in 1988 to replace and standardize organizational and individual messaging systems over 20 years.[2] DMS was to replace the Automated Digital Network (AUTODIN) which was DoD unique, inefficient, obsolete and too expensive to maintain. In reality, DMS subsumed AUTODIN. To this day DMS continues to use and maintain AUTODIN communications links, but DoD renamed them as legacy DMS links. DMS met its goal of standardizing organizational messaging using International Telecommunications Union (ITU) X.400 and X.500 protocols. The X.400-series ITU recommendations specify standard protocols for exchanging and addressing electronic messages. X.500 is a series of computer networking standards covering electronic directory services. These standards enable DoD organizations with DMS to communicate with each other as well as with inter-agency, allied, North Atlantic Treaty Organization (NATO) entities and other organizations. In short, the Defense Message System is an email system. While some would argue that DMS is a more rigorous form of email it is email nonetheless.

DMS was conceived because email was cost effective, because the large number of email systems within DoD did not interoperate with each other, and because modern doctrines of force deployment developed in conflicts during the 1980s demanded a broader range of messaging services.[3] These reasons served as the impetus for change in 1988 and they still serve as the reasons for modernizing the organizational messaging capability within DoD today.

Applying the reasons for building DMS in the current environment sheds some light on why change is required. While email is a cost effective method of transmitting information, the DMS implementation of email is not. DMS has a budget of approximately 600 million dollars across the Future Years Defense Program (FYDP) or 120 million dollars per year. With an account base of 20,230 DMS spends roughly 5,931 dollars per account.[4] By contrast, the newly announced enterprise email program will have an initial account base of 1.5 million spending approximately fifty dollars per account.[5] Granted, the enterprise email program does not have the same requirements as DMS but the cost difference is staggering. The DMS system treats all messages equally regardless of the information being sent unnecessarily increasing the cost. A simple analogy might be driving an M1A2 Abrams main battle tank to do routine tasks when a High-Mobility Multipurpose Wheeled Vehicle (HMMWV) is available.

DMS is not interoperable with other email systems in DoD or the remainder of the United States. Most US email systems today use Simple Mail Transfer Protocol (SMTP) while DMS uses X.400. Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission across Internet Protocol (IP) networks.[6] In a March 1, 2000 Industry Advisory Panel report on the Defense Message System

way ahead, the panel recommended transitioning from the X.400 protocol to SMTP and PKI.[7] There is no reluctance on the part of the DMS program office to move to SMTP and PKI.[8] When the Joint Staff, using a Joint Staff Action Package (JSAP), coordinated with the Allies requesting information on the impact of closing DMS they each responded via email, not DMS. Significantly, there are also many other information transfer methods available to the warfighter; SharePoint, wikis, blogs, chat, Facebook, Twitter, etc. Most of these technologies are cheaper, faster and more user friendly. Command and Control (C2) messages are routinely transmitted in chat rooms throughout Iraq and Afghanistan. Unfortunately they are not interoperable with DMS.

Due to changing doctrines and force deployments the last reason for change was a demand for broader messaging services. Since the establishment of DMS, the Services in general and the Army in particular have undergone complete transformations in both force structure and doctrine. The Cold War was an age of large formations and set piece battles. Units received and sent information hierarchically in stovepipes to their higher headquarters. On the modern battlefield these Cold War stovepipes are ineffective. The Cold War model tended to send information along the chain of command. In order to gain a more accurate picture of their environment, commanders at all levels share information not just vertically but also horizontally. This model makes information available where it is needed, transmitting along the chain of information versus the chain of command. Modularity gives Army the flexibility to tailor combat forces to meet the mission requirements. The Air Forces and Marine Corps are similarly modular. Commanders in Iraq and Afghanistan rarely use DMS to transfer information and if they do it is a secondary or tertiary means of communication.

Commands to engage the enemy are sent in chat channels, orders are disseminated on SharePoint pages and wikis are used to collaborate on topics. DMS has not kept pace with the changes in doctrine or force structure and deployment. While the DMS program office is responsive to new capabilities, the problem lies with the system itself. The system is monolithic, more difficult to use than other transmission media, cumbersome to change and expensive to maintain. The information must have the capability to be rapidly accessed from any place at any time. It needs the ability to be shared with the unintended authorized user. Commanders and units on the modern battlefield have moved to a network and information centric model for messaging while DMS remains mired in its system approach. Organizational messaging needs to fit into how the Department fights and wins the nation's wars now, not how it fit into how the Department organized and prepared to fight during the Cold War.

The Department of Defense has recognized that DMS is at end of life. On 16 May 2005, the Office of the Assistant Secretary of Defense (ASD), specifically the Office of Networks and Information Integration (NII), released a memorandum directing the Defense Message System be placed into sustainment, removing DMS from the Information Technology Acquisition Program (ITAP) List and issuing an end to the program for Fiscal Year (FY) 2012.[9] In September 2008 the DoD Chief Information Officer (CIO) confirmed the sustainment of DMS and the intent to transition Organizational Messaging to a net-centric environment.[10] The Vice Chairman of the Joint Chiefs of Staff, General Cartwright, sent a memorandum to the Service Chiefs and the Combatant Commanders announcing his intention to eliminate DMS in fiscal year 2009 and employ alternative mechanisms for the transfer of Official Information (OI).[11]

Recognizing the need to stay aligned with the capability and not system even the DMS program office has been designated the Organizational Messaging Division.[12]

The reasons for failure to eliminate DMS in FY 2009 are not technical, but cultural. FY 2012 is right around the corner and there is no effort to transition to a new organizational messaging paradigm. In fact, DMS will continue to receive funding. In a memorandum to Secretaries of the Departments, the acting director for ASD-NII stated that all funding lines identified as "DMS" must be preserved to fund a deliberate transition to successor OI capabilities as well as sustain mission critical services such as Focal Point, Nuclear Command, Control, Communications and communications with Allies until alternatives are available.[13] Lack of direction from OSD keeps the program from moving forward.[14] This relieves the pressure on the program office to transition from DMS and continues the status quo. The memorandum also states that DMS should be simplified through regionalization and virtualization of DMS services and that this process should continue through 2014.[15] Not only is the focus is on the system rather than the information but there is acknowledgement that the Defense Message System will continue well beyond its approved End of Life date. On one hand, there are existing embedded mechanisms for change, and on the other hand the reinforcing mechanisms for change are missing.

Requirements

In part, the difficulty of eliminating DMS lies with the current requirements. The requirements are spelled out in the Multicommand Required Operational Capability (MROC) 3-88 for the Defense Message System, 1 October 1997, with Change 2.[16] The original requirements were written in 1988 and validated by the Joint Staff in February 1989[17] without much change since then. They are:

- Connectivity/Interoperability
- Message Delivery
- Timely Delivery
- Confidentiality/Security
- Sender Authentication
- Integrity
- Availability/Reliability
- Training
- Identification of Recipients
- Message Preparation Support
- Storage and Retrieval Support
- Distribution Determination and Delivery

Advances in networking and technology have badly dated some of the requirements while others are not being met or met with caveats. In other cases it has enhanced DMS capability beyond the original requirement. Reviewing the requirements briefly will help better describe what next generation organizational messaging needs may be.

Connectivity/Interoperability. In short, an authorized user should be able to communicate with any other user within the community. It should provide standard interfaces to other Government agencies, allies, defense contractors, and other approved activities external to the DMS community. System users may be fixed, mobile, or transportable. The DMS must be interoperable with tactical data distribution systems. The DMS must also be interoperable with and provide standard interfaces for

allied systems.[18] In the early days of networking not all e-mail systems were equal or interoperable. The same can be said of the networks themselves with different routing protocols unable to communicate with one another. Organizational messaging was originally standardized on X.400, the International Telecommunication Union standard for Data Communication Networks for Message Handling Systems (MHS) — or e-mail, partly because it integrated integrity and security features before they were available in Simple Mail Transfer Protocol (SMTP) and federal mandates to use OSI protocols.

Message Delivery. The system must, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message, a method of promptly notifying the sender of the non-delivery must be available. It should provide message accountability and traceability from writer to reader.[19] The current Defense Information System Agency (DISA) standard for message delivery is 98%.[20] The self-imposed 98% delivery standard is rarely met within DoD. As indicated by statistics briefed at the monthly DMS Operations Group meetings which range from 99% to 35%. A majority of non-delivery notifications are due the processes the system uses and is not an accurate representation of DMS message delivery. An example is an incorrectly addressed message; it will not reach its non-existent destination and so generate a non-delivery notification. The wrong metrics, or the inability to measure them correctly, are currently being used to gage success for this requirement. However, if 98% is the message delivery standard then almost any messaging system is good enough for organizational messaging. As technology in general and networking in particular has become more reliable this requirement is in need of modification.

Timely Delivery. This requirement refers to how fast a message arrives at its destination. It is commonly called the precedence requirement. The MROC requires support for at least two levels of precedence determined by the originator. Commanders want the ability to send a FLASH, IMMEDIATE, PRIORITY or ROUTINE messages. What commanders do not always know are the metrics for the levels of precedence. The Allied Communication Publication (ACP) 123 defines the following: a FLASH message must arrive within ten minutes, IMMEDIATE 20 minutes, PRIORITY 45 minutes, and a ROUTINE message must arrive within 8 hours or next duty day. These are antiquated standards and irrelevant in the world of Internet Protocol (IP). When the servers are up and links are connected all messages arrive well within 10 minutes of sending, most within seconds, making every message a FLASH message.

Confidentiality/Security. The requirement to process and protect all traffic at appropriate security levels and compartments. This is nothing more than approved encryption for required messages. Currently Fortezza® cards are used to secure messages.[21] Fortezza® cards are Personal Computer Memory Card International Association (PCMCIA) cards that contain the user's private key.[22] These cards are similar in nature to the DoD Common Access Cards (CAC) as they use a Public Key Infrastructure (PKI) public-private key pair to affect confidentiality, security and integrity. Public Key Infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[23] The difference between Fortezza® and CAC cards is the strength of the encryption algorithm.

Sender Authentication. This is the non-repudiation requirement. More plainly stated it is the ability to unambiguously verify that the stated originator did in fact originate the message. This requirement is also achieved through Fortezza® and PKI public-private key pairs. This capability already exists within other DoD messaging systems and can be implemented using current Common Access Cards already in possession by all DoD employees. An example is the Army Knowledge Online / Defense Knowledge Online single sign-on service. This net-centric service uses DoD CAC cards to authenticate users for many applications across the Department of Defense. The single sign-on service is easily integrated into applications and alleviates the need for local account management.

Integrity. Information received must be the same as information sent.[24] The message must be unaltered. Security classification, addressing, routing and auditing must be safeguarded by the system. Confidentiality, sender authentication and integrity are achieved using Public Key Infrastructure (PKI) and Fortezza® cards. This requirement is met by using the Secure Hash Algorithm (SHA) to hash the message prior to transmission.[25] A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value.[26] The hash is called a message digest. The message digest is then attached to the message and sent to its destination. Once at the destination the message is hashed again with the same algorithm and the results compared to ensure the message is unaltered. The cryptologic algorithm only works in one direction so the contents of the message cannot be ascertained from the message digest and works in

such a way that no two messages can have the same message digest. As with the sender authentication requirement, this capability already exists and is implemented using current Common Access Cards already in possession by all DoD employees.

Availability/Reliability. Provide users with message service on an essentially continuous basis. The required availability should be achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.[27] Most computer systems and services rely on power and the network, especially in current net-enabled, net-centric environment. Failure of either will degrade or disrupt message service to authorized users.

Training. Training must be flexible and responsive enough to allow user operation without extensive training. System training shall be developed and provided for system users and support personnel.[28]

Identification of Recipients. The sender must be able to unambiguously identify the intended recipient organizations.[29] This requirement is nothing more than a global address book. Current efforts such as the Joint Enterprise Directory Service (JEDS) can easily provide this service without integration into a system.[30] JEDS is a newly started enterprise-wide directory service that provides DoD People Discovery (i.e. white pages) and DoD identity management attribute services to support DoD access control decisions.[31]

Message Preparation Support. The DMS must support user-friendly preparation of messages for transmission, and allow the use of external message editors.[32] This requirement is currently met with the United States Message Text Format (USMTF). Contrary to popular belief, USMTF no longer requires capitalization of an organizational

message. Capitalizing the entire message is a legacy practice that is culturally ingrained with organizations and services equating capitalization of the message to official-ness. A brief discussion on official information follows later.

Storage and Retrieval Support. DMS must support storing messages after delivery to allow retrieval for such purposes as forwarding, resending and supporting automated message handling functions. The minimum storage period for organizational messages will be specified by Allied Communications Procedures (ACP).[33] The current standard in the ACP is ten days. Messages are routinely held much longer than the required ten days, sometimes in excess of seven years. Here again the requirement is obsolete. Commanders at all levels require information retention of much longer than ten days. This is one area where DMS has excelled and exceeded the requirement by three orders of magnitude.

Distribution Determination and Delivery. Provide the message originator with the capability to specify special handling and delivery instructions. Distribution lists also fall under this requirement. As the MROC states these requirements will be satisfied procedurally and not levied as a technical or system requirement this requirement has no impact on the obsolescence of DMS.

In February 2009 the Joint Staff asked the Combatant Commanders, Services and Agencies (C/S/A) to validate the MROC requirements. C/S/As made the argument that current requirements cannot be cost effectively met using newer technologies and so DMS remains the status quo. The MROC requirements pertain to all messages (information) and DMS is the only system capable of meeting all requirements. But messaging is not about the system, it is about the information. Not all information

requires that all twelve MROC requirements are levied against them. Certainly security and non-repudiation are not requirements for an administrative message to subordinate units.

Culture

Organizational culture is another major barrier to gaining support for information centric organizational messaging. It is very hard to eliminate or change a program as institutionally entrenched as DMS. When working groups and tiger teams are chartered to discuss DMS transition the Services and Combatant Commands naturally send their messaging experts, most of which are DMS related personnel. These DMS personnel, both government and contractor, have a vested interest in the continuation of DMS as a program of record. There is some validity in saying that if the DMS program is eliminated the contracts associated with the program will also be eliminated. The Military Communications Electronics Board (MCEB) recognized this challenge and responded by disbanding the Organizational Messaging Working Group (OMWG) in hopes of getting the right stakeholders to the table on the issue of transitioning organizational messaging off of DMS. This is the first of many cultural barriers inhibiting change in the organizational messaging arena. The new working group chartered to examine the organizational messaging issue is the Official Information Exchange working group. Unfortunately it contained many of the same members as the original OMWG.

Anecdotally, the Navy will not move a ship without a DMS message. They may already have the information from multiple other sources but they will not move the ship until they have a message from the DMS system. The Navy, as well as other Services, claims the information is not official until it is received via DMS. While this is their view

as seen through their cultural lens, it is not fact. The definition of official information was the subject of great debate among the Services between March and June 2009.

DoD created a Tiger Team comprised of representatives from the services, agencies and Combatant Commands co-chaired by ASD(NII) and the United States Strategic Command (USSTRATCOM) to gain clarity and consensus on the definition of official information. The final verbiage is the Joint Publication 1-02 definition, "Information that is owned by, produced for or by, or is subject to the control of the United States Government."[34] This definition is not confined to the DMS system. Quite the contrary, any information generated on any government owned computer is considered official so an email or a wiki entry may also be official. There is no mention of official information in Chairman's Joint Chiefs of Staff Instruction (CJCSI) 5721.01E, Defense Message System. The instruction describes only organizational messaging. By extension, as DMS messages are generated on a government owned system the messages are official, but that does not preclude other transmission means from being official as well. The pattern continues; messaging is not about the system generating the information, it is about the information.

The Art of the Possible

In August 2009, The Joint Staff conducted an exercise to determine what was possible given no additional resources. The intent was to determine the low hanging fruit and what was hard to do in the organizational messaging arena. On average, the Joint Staff originated 900 messages a month.[35] After review, these messages were lumped into four categories; test, general administration, individual message and orders. Test messages were messages that were sent from point to point to determine

if the system was operating properly. General administration, individual and orders messages are exactly as stated.

The DMS sundown exercise, as it came to be known, was conducted in 4 phases over 4 months in 2009. In May, the Joint Staff eliminated test messages. In June, the Vice Chairman directed the Joint Staff to send general administration, or GENADMIN, messages using alternative means. In July, the Joint Staff moved individual messages to alternative means and finally in August 2009, orders were moved off of the DMS system. The only messages permitted to be sent via DMS were Nuclear C3 and Focal Point/Alternative or Compensatory Control Measures specifically allowed by the Vice Chairman's memorandum.[36] The end result was that the Joint Staff went from sending an average of over 900 messages per month in the beginning of the year to only sixteen in August 2009.[37] Of the remaining sixteen messages seven should have been sent using alternative mechanisms leaving nine messages in the "hard to do" category. As it turned out, not much had to change to eliminate those messages from DMS. Many of the messages were duplications of information already sent and were resent on DMS because an instruction, a local policy directed the information be sent on DMS or that it had always been done that way. Changes to the instructions, policy or process were made and codified to reduce DMS usage. For instance, whenever a Joint Staff Action Package was sent to the Combatant Commanders a DMS message would follow. This local requirement duplicated the information and was unnecessary. Another duplication of information was the process for theater clearances requests for official overseas travel. The policy required a DMS message when the information was already required by the Automated Personnel & Aircraft Clearance System (APACS). In most cases

organizations welcomed the opportunity to stop using DMS. The elimination of duplicative messages was welcome by all organizations. The lack of centralization was the main complaint.

Proposal for Change

So what should the DoD's information centric organizational messaging system look like? First and foremost it needs to fit into the architecture of the future. This architecture is described by both the DoD CIO and the Joint Staff J6 in the Defense Information Environment (DIE) and the Global Information Grid 2.0 (GIG 2.0) respectively. Key are the five attributes of GIG 2.0.[38]

- Global Authentication, Access Control and Directory Services
- Information and Services "from the edge"
- Joint Infrastructure
- Common Policies and Standards
- Unity of Command

The next generation organizational messaging must live within this framework and will be dependent on other efforts. Identity management, Joint Enterprise Directory Service (JEDS) and Service Oriented Architecture (SOA) Enterprise Service Bus (ESB) efforts are examples of requirements that will impact next generation organizational messaging. If these efforts are successful it will be easy to build the next messaging platform of the future that is cheaper, more reliable, and has greater flexibility while still meeting the needs of the war-fighter.

In its current form organizational messaging is centralized and hierarchical. Assuming that the current efforts of identity management, Joint Enterprise Directory

Service and Joint User Messaging are successfully implemented, the way to an information centric organizational messaging platform is to break up the Multicommand Required Operational Capability (MROC) requirements into individual services. In Ori Brafman and Rod A. Beckstrom view, the Defense Message System would be a spider.[39] What organizational messaging needs to become is a starfish. Decoupling the requirements from the system will allow the user to determine what his or her needs are for the information being sent. While an operations order may still have the need for all of the requirements, the message regarding the Army's Birthday will not. Decoupling the requirements from the system will also allow for more flexibility as changing any one of the services will not require a change to the others. With GIG 2.0 providing authentication, access control and directory services four of twelve MROC requirements are met. The messaging service would be net-centric so it would not require any specialized user equipment. Imagine logging into the messaging service with a Common Access Card (CAC). Many users already accomplish this by logging into DMS via AMHS. With this action the user has accomplished sender authentication. If we make use of the CAC Public Key Infrastructure certificates resident on the card we can also accomplish confidentiality, security, and integrity. JEDS provides the identification of recipients with its enterprise directory. These services exist today and need not be duplicated in a messaging system. Each of these services/requirements should be a check box in the messaging service that can be selected the user. Other checkboxes for message delivery and other services could be added as well. Storage and retrieval could easily be accomplished in this way as well. If the user believes the message needs to be retained the appropriate box is checked and a courtesy copy of the

message is sent to a repository system. This system would publish the message and have search functionality. Decoupling the requirements from a system allows greater flexibility for the infusion of new technologies as only the applicable service need be changed versus a system with all of its associated interdependencies.

The new approach needs to be evolutionary rather than revolutionary. There is a wealth of knowledge in the Organizational Messaging Division that should be leveraged in order to develop the best possible next generation messaging system. The agile development method is ideally suited to transform DMS to its successor.

Such an information centric messaging methodology would have many advantages over the current system centric approach. In all fairness, there would also be some risk. The hard to do messages must still be dealt with. They boil down to two types of messages, the first type is to submerged submarines and the second type is to Allies and NATO. These challenges would be dealt with similarly. The information would be converted to the format required of the receiving system. DMS does this today already for submarines. It would only require a change in the programming of the existing Tactical Messaging Gateway (TMG) or Multi-function Interpreter (MFI). A similar change in programing would be required in the National Gateways for information sent to the Allies and NATO. The TMG, MFI and National Gateways convert the message into a format that can be read by the intended recipient.

DMS is a fire and forget system. Once a message is in the system it will be delivered to the desired recipients without any user interaction. The program office likens it to a newspaper delivery service, the message will get to the front door, all that is required is that you open it and retrieve your message. This message delivery

assurance is the most expensive part of DMS as it is accomplished through the use of a large number of contractors who will troubleshoot any non-delivery notification until the issue is resolved. In order to realize the cost savings DoD would want of the new information centric organizational messaging platform the user would have to play a greater role in messaging and be responsible more for their messages. In order to eliminate cost users would have watch their boxes for non-delivery notifications and either resend or find alternate means to transmit the information. Again, users would have to become more responsible for their messages.

Conclusion

Messaging is about the information, not the system. The current organizational messaging capability within the Department of Defense is an old technology operating on an obsolete paradigm. Organizational messaging must shift to an information centric versus a system centric paradigm. Not only is an information centric paradigm cheaper to maintain, it is also more flexible and easier to modify. Most information is already available to the user in forms other than a DMS message. Promotion and other board results are posted to web pages; we receive messages through email by subscribing to lists such as S1NET and STAND-TO!; information is entered into specialized systems such as APACS; commands are sent via chat channels; information is posted on social media forums such as Facebook and Twitter. Defense Message System is obsolete compared to these other information platforms. With Defense Message System end of life near the Department of Defense has an opportunity to shift messaging to a service type platform decoupling the requirements from the system in the process.

Endnotes

[1] Vice Chairman of the Joint Chiefs of Staff James E. Cartwright, "Use of Defense Message System (DMS) for Official Information (OI) Transfer" memorandum for the Service Chiefs and Combatant Commanders, Washington, DC, November 26, 2008

[2] G.F. Hice and S.H. Wold, DMS: Prologue to the Government E-Mail Revolution (Centerville: J.G. Van Dyke & Associates, Inc.), 1

[3] Ibid., 3-4

[4] Brian Ives, "DMS Transition," briefing slides with commentary, Fairfax, VA, DMS Operations Group, January 13, 2011.

[5] Stephen Simpkins, email message to Enterprise Email blog, February 2, 2011.

[6] Simple Mail Transfer Protocol, December 24, 2010, linked from Wikipedia home page, http://en.wikipedia.org/wiki/Smtp (accessed December 28, 2010).

[7] Unknown, "Defense Message System Way Ahead, Conclusions and Recommendations from the Industry Advisory Panel", March 1, 2000, 3.

[8] William Arey, Organizational Messaging Division Lead Engineer, interview by author, Arlington, VA, January 26, 2011.

[9] Assistant Secretary of Defense Linton Wells II, "Defense Message System (DMS); Removal from Information Technology Acquisition Program (ITAP) List" memorandum for Secretaries of the Military Departments, Washington, DC, May 16, 2005.

[10] Department of Defense Chief Information Officer John G. Grimes, "Organizational Messaging Transition" memorandum to Chief Information Officers of the Military Departments, Washington, DC, September, 19 2008.

[11] Vice Chairman of the Joint Chiefs of Staff James E. Cartwright, "Use of Defense Message System (DMS) for Official Information (OI) Transfer" memorandum for the Service Chiefs and Combatant Commanders, Washington, DC, November 26, 2008.

[12] William Arey, Organizational Messaging Division Lead Engineer, interview by author, Arlington, VA, January 26, 2011.

[13] DoD Deputy Chief Information Officer, David M. Wennegren, "Strategy for Defense Message System (DMS) Migration to Official Information (OI) and Organizational Messaging (OM) Service Oriented Enterprise Solutions" memorandum for Secretaries of Military Departments, Washington, DC, January 6, 2010.

[14] Director Defense Information Systems Agency, Lieutenant General Carroll F. Pollett, "Strategy for Defense Message System (DMS) Migration to Official Information (OI) and Organizational Messaging (OM) Service Oriented Enterprise Solutions" memorandum for the Department of Defense Chief Information Officer, Arlington, VA, March 31, 2010.

[15] DoD Deputy Chief Information Officer, David M. Wennegren, “Strategy for Defense Message System (DMS) Migration to Official Information (OI) and Organizational Messaging (OM) Service Oriented Enterprise Solutions” memorandum for Secretaries of Military Departments, Washington, DC, January 6, 2010.

[16] Director for Command, Control, Communications and Computer Systems Lieutenant General Douglas D. Buchholz, “Change 2 to Multicommand Required Operational Capability (MROC) 3-88, The Defense Message System (DMS)” memorandum for Service Chiefs, Combatant Commanders and Agencies, Washington, DC, October 1, 1997, 1

[17] Hice and Wold, DMS: Prologue to the Government E-Mail Revolution, 6

[18] Director for Command, Control, Communications and Computer Systems Lieutenant General Douglas D. Buchholz, “Change 2 to Multicommand Required Operational Capability (MROC) 3-88, The Defense Message System (DMS)” memorandum for Service Chiefs, Combatant Commanders and Agencies, Washington, DC, October 1, 1997, 13

[19] Ibid., 13-14

[20] William Arey, Organizational Messaging Division Lead Engineer, interview by author, Arlington, VA, January 26, 2011.

[21] Hice and Wold, DMS: Prologue to the Government E-Mail Revolution, 33

[22] Ibid.

[23] Public key infrastructure, 8 December 2010, linked from Wikipedia home page, http://en.wikipedia.org/wiki/Public_key_infrastructure, (accessed December, 16 2010).

[24] Director for Command, Control, Communications and Computer Systems Lieutenant General Douglas D. Buchholz, “Change 2 to Multicommand Required Operational Capability (MROC) 3-88, The Defense Message System (DMS)” memorandum for Service Chiefs, Combatant Commanders and Agencies, Washington, DC, October 1, 1997, 17.

[25] Hice and Wold, DMS: Prologue to the Government E-Mail Revolution, 34

[26] Unknown, “Cryptographic hash functions”, February 26, 2011, linked from the *Wikipedia Home Page* at http://en.wikipedia.org/wiki/Cryptographic_hash_function (accessed February 28, 2011).

[27] Director for Command, Control, Communications and Computer Systems Lieutenant General Douglas D. Buchholz, “Change 2 to Multicommand Required Operational Capability (MROC) 3-88, The Defense Message System (DMS)” memorandum for Service Chiefs, Combatant Commanders and Agencies, Washington, DC, October 1, 1997, 18.

[28] Ibid., 19.

[29] Ibid.

[30] Unknown, “DISA Enterprise Directory Service: GDS and JEDS”, n.d. linked from the *DISA Home Page* at http://www.disa.mil/services/gds.html (accessed February 28, 2011).

[31] Ibid.

[32] Director for Command, Control, Communications and Computer Systems Lieutenant General Douglas D. Buchholz, “Change 2 to Multicommand Required Operational Capability (MROC) 3-88, The Defense Message System (DMS)” memorandum for Service Chiefs, Combatant Commanders and Agencies, Washington, DC, October 1, 1997, 20.

[33] Ibid., 21.

[34] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: Joint Chiefs of Staff, April 12, 2001 as amended through July 31, 2010), 336

[35] Edward C. Prem, “DMS Sundown Exercise,” briefing slides, Pentagon, Washington DC, Official Information Exchange Working Group, February, 2009.

[36] Vice Chairman of the Joint Chiefs of Staff James E. Cartwright, “Use of Defense Message System (DMS) for Official Information (OI) Transfer” memorandum for the Service Chiefs and Combatant Commanders, Washington, DC, November 26, 2008

[37] Edward Prem, “DMS Update,” briefing slides with commentary, Pentagon, Washington, DC, Vice Chairman of the Joint Chiefs of Staff Update, August 2009.

[38] GIG 2.0 Operational Reference Architecture, linked from Intelipedia home page, https://www.intelink.gov/wiki/Global_Information_Grid_2.0, (accessed December 16, 2010)

[39] O. Brafman and R. Beckstorm, The Starfish and the Spider (New York: Penguin Group, 2006)